

Rank equivalent and rank degenerate skew cyclic codes

Umberto Martínez-Peñas *

Department of Mathematical Sciences, Aalborg University, Denmark

January 27, 2016

Abstract

Two skew cyclic codes can be equivalent for the Hamming metric only if they have the same length, and only the zero code is degenerate. The situation is completely different for the rank metric, where lengths of codes correspond to the number of outgoing links from the source when applying the code on a network. We study rank equivalences between skew cyclic codes of different lengths and, with the aim of finding the skew cyclic code of smallest length that is rank equivalent to a given one, we define different types of length for a given skew cyclic code, relate them and compute them in most cases. We give different characterizations of rank degenerate skew cyclic codes using conventional polynomials and linearized polynomials. Some known results on the rank weight hierarchy of cyclic codes for some lengths are obtained as particular cases and extended to all lengths and to all skew cyclic codes. Finally, we prove that the smallest length of a linear code that is rank equivalent to a given skew cyclic code can be attained by a pseudo-skew cyclic code. Throughout the paper, we find new relations between linear skew cyclic codes and their Galois closures.

Keywords: Cyclic codes, Galois closure, linearized polynomial rings, network coding, rank degenerate, rank distance, rank equivalence, skew cyclic codes.

MSC: 15B33, 94B15, 94B65.

1 Introduction

Codes in the rank metric have numerous applications, such as network coding [10, 13, 16] or cryptography [7]. Among these codes, cyclic codes and skew cyclic codes have been considered in [1, 2, 4, 5, 6, 7, 12], since they have simple algebraic descriptions and fast encoding and decoding algorithms.

In the network coding model of [10, 13, 16], the length of a rank-metric code corresponds to the number of outgoing links from the source or the number of packets needed to be sent by the source. Whereas it is obvious how to increase the length of a code and preserve at the same time its rank-metric properties, just by appending zeroes, it is

*umberto@math.aau.dk

not obvious whether a rank-metric code can be shortened (which would mean that it is degenerate) nor how. On the other hand, skew cyclic codes of smaller length have faster encoding and decoding algorithms.

In contrast with the Hamming-metric case, skew cyclic codes may be rank equivalent and have different lengths. Moreover, many non-zero skew cyclic codes are rank degenerate.

The aim of this paper is to study rank equivalences between skew cyclic codes, focusing on equivalences that commute with the shifting operators, and study in which way skew cyclic codes can be rank degenerate.

Both problems have direct consequences on the generalized rank weights [10] of skew cyclic codes, which measure the information leakage by wiretapping links in the network, following the model of [10, 13, 16]. In particular, from our study we will obtain as particular cases the main results in [4], which give exact characterizations of cyclic codes with minimal generalized rank weights by means of their root sets when their length and field size are coprime. Our results have such consequences for all lengths, do not require computing roots (or may require computing roots of linearized polynomials, which can be done efficiently) and can be applied to all skew cyclic codes.

After some preliminaries in Section 2, the results in this paper are as follows: in Section 3, we define different types of length for skew cyclic codes, regarding the rank metric, and establish some inequalities between them. In Section 4, we use the polynomial description of the Galois closure of skew cyclic codes to compute most of the lengths defined in the previous section. In Section 5, we treat cyclic codes and relate their polynomial description to that of their Galois closures (by means of generator and check polynomials, idempotent generators and root sets), giving at the end several characterizations of rank degenerate cyclic codes and obtaining the results in [4] as particular cases. In Section 6, we proceed as in the previous section, but for general skew cyclic codes, using their linearized-polynomial description. Finally in Section 7, we see that, although the linear code of minimum length that is rank equivalent to a given skew cyclic code need not be skew cyclic, it may be chosen as pseudo-skew cyclic in many cases.

2 Definitions and preliminaries

Fix a prime power q and positive integers m and n , and let \mathbb{F}_{q^s} denote the finite field with q^s elements for a positive integer s . A code $C \subseteq \mathbb{F}_{q^m}^n$ will be called linear if it is \mathbb{F}_{q^m} -linear. In general, linearity will mean \mathbb{F}_{q^m} -linearity. The number n is called the length of the code C .

We will denote the coordinate indices in $\mathbb{F}_{q^m}^n$ from 0 to $n-1$, and consider them as integers modulo n . Given a vector $\mathbf{c} \in \mathbb{F}_{q^m}^n$, we define its rank weight [5] as the dimension of the \mathbb{F}_q -linear vector space generated by its components. We denote it by $\text{wt}_R(\mathbf{c})$.

Define the shifting operator $s_n : \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_{q^m}^n$ as

$$s_n(c_0, c_1, \dots, c_{n-1}) = (c_{n-1}, c_0, \dots, c_{n-2}),$$

for every $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_{q^m}^n$. For any integer $r \geq 0$, define also the r -th

Frobenius and q^r -shifting operators as $\theta_r, \sigma_{r,n} : \mathbb{F}_{q^m}^n \rightarrow \mathbb{F}_{q^m}^n$, respectively, where θ_r acts by raising every component of a vector to the power q^r and $\sigma_{r,n} = \theta_r \circ s_n$.

Definition 1. A code $C \subseteq \mathbb{F}_{q^m}^n$ is cyclic if $s_n(C) \subseteq C$, is q^r -cyclic (or skew cyclic of order r) if $\sigma_{r,n}(C) \subseteq C$, and is Galois closed (over \mathbb{F}_q) if $\theta_1(C) \subseteq C$.

Observe that cyclic codes are q^0 -cyclic (or q^m -cyclic), that is, they are also skew cyclic. Skew cyclic codes were introduced in [5] for $r = 1$ and $n = m$, and then independently in [6] for $r = 1$ and in [1] for general parameters.

Denote $[i] = q^i$, for any integer $i \geq 0$. Following [17], for a given linear code $C \subseteq \mathbb{F}_{q^m}^n$, we define its Galois closure as $C^* = \sum_{i=0}^{m-1} C^{[i]}$, which is the smallest linear Galois closed space containing C , and we also define $C^0 = \bigcap_{i=0}^{m-1} C^{[i]}$, which is the biggest linear Galois closed space contained in C . Recall from [17, Lemma 2] that $(C^\perp)^* = (C^0)^\perp$ and $(C^\perp)^0 = (C^*)^\perp$.

On the other hand, if $V \subseteq \mathbb{F}_{q^m}^n$ and $V' \subseteq \mathbb{F}_{q^m}^{n'}$ are linear Galois closed spaces, we say that a map $\phi : V \rightarrow V'$ is a rank equivalence if it is a vector space isomorphism and $\text{wt}_R(\phi(\mathbf{c})) = \text{wt}_R(\mathbf{c})$, for all $\mathbf{c} \in V$. We say that two codes C and C' are rank equivalent if there exists a rank equivalence between linear Galois closed spaces V and V' that contain C and C' , respectively. This definition of rank equivalent linear codes was introduced in [13, Definition 5].

By [13, Theorem 5], rank equivalent codes not only perform exactly in the same way regarding rank error and erasure correction, but also information leakage on networks (see [13, Remark 5]). Moreover, rank equivalences can be easily described, as the following lemma states, which is a particular case of [13, Theorem 5]:

Lemma 1. A vector space isomorphism $\phi : V \rightarrow V'$ between linear Galois closed spaces is a rank equivalence if, and only if, there exist $\beta \in \mathbb{F}_{q^m}^*$ and an $n \times n'$ matrix A over \mathbb{F}_q that maps bijectively V to V' and such that

$$\phi(\mathbf{c}) = \beta \mathbf{c} A,$$

for all $\mathbf{c} \in V$.

As in [13, Definition 6], we say that a linear code $C \subseteq \mathbb{F}_{q^m}^n$ is rank degenerate if it is rank equivalent to a linear code with smaller length (see also [9] for an alternative equivalent definition of rank degenerate codes). In network coding this means that the code C may be implemented (with the same performance) on a network with less outgoing links or where the source needs to send less packets [13, 16].

3 Lengths and Galois closures

Following the model in [10, 13, 16], given a linear code $C \subseteq \mathbb{F}_{q^m}^n$, the length n represents the number of outgoing links of a network where C is implemented, or the number of packets needed to be sent from the source, whereas m represents the packet length. If C is rank equivalent to a code with length $n' \neq n$, then it may be implemented as a linear

code in a network with n' outgoing links and with exactly the same performance [13]. However we may want to implement C as a skew cyclic code, and hence we need it to be rank equivalent to a skew cyclic code of length n' .

On the other hand, encoding and decoding of skew cyclic codes is faster if the length is smaller, and we may always increase their lengths preserving their rank-metric properties just by appending zeroes on the right of each codeword.

This motivates the following definitions:

Definition 2. Given a linear code $C \subseteq \mathbb{F}_{q^m}^n$, an element $a \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ and an integer $r \geq 0$, we define the following numbers:

1. The rank length, $l_R(C)$, as the minimum n' such that C is rank equivalent to a linear code of length n' .
2. The r -th skew length, $l_{Sk,r}(C)$, as the minimum n' such that C is rank equivalent to a linear skew cyclic code of order r and length n' , if such a code exists. We define $l_{Sk,r}(C) = \infty$ otherwise.
3. The (a, r) -shift length, $l_{Sh,a,r}(C)$, as the minimum n' such that C is rank equivalent to a linear code of length n' by a rank equivalence ϕ such that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$, if such a code exists. We define $l_{Sh,a,r}(C) = \infty$ otherwise.
4. The period length, $l_P(C)$, as the minimum integer $1 \leq p \leq n$ that generates the ideal modulo n defined as $\{p' \mid c_{i+p'} = c_i, \forall i, \forall (c_0, c_1, \dots, c_{n-1}) \in C\}$, which necessarily divides n .

We also say that an integer $1 \leq p \leq n$ is an a -period of C if $c_{i+p} = ac_i$, for all $i = 0, 1, 2, \dots, n-1$ and all $(c_0, c_1, \dots, c_{n-1}) \in C$.

Remark 1. In the definition of $l_{Sh,a,r}(C)$, the rank equivalence ϕ that commutes with the q^r -shifting operators is supposed to be defined between linear Galois closed spaces that are cyclic, in order to make sense (see Lemma 2 below).

Remark 2. Assume that V and V' are linear cyclic Galois closed spaces. If a rank equivalence $\phi : V \rightarrow V'$ satisfies that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$, for some $r \geq 0$ and $a \in \mathbb{F}_q^*$, then

$$\begin{aligned} \phi(\sigma_{s,n}(\mathbf{c})) &= \beta^{1-[s-r]}(\beta\sigma_{r,n}(\mathbf{c})A)^{[s-r]} \\ &= \beta^{1-[s-r]}(a\sigma_{r,n'}(\phi(\mathbf{c})))^{[s-r]} = (\beta^{1-[s-r]}a)\sigma_{s,n'}(\phi(\mathbf{c})), \end{aligned}$$

for all $\mathbf{c} \in V$, where A and β are as in Lemma 1. Hence, ϕ sends q^s -cyclic codes to q^s -cyclic codes, for any $s \geq 0$.

We have the following on the skew cyclic structure of linear Galois closed spaces:

Lemma 2. If $V \subseteq \mathbb{F}_{q^m}^n$ is linear and Galois closed, then it is skew cyclic of some order if, and only if, it is skew cyclic of all orders. Given a linear code $C \subseteq \mathbb{F}_{q^m}^n$, if it is skew cyclic of some order, then C^* and C^0 are skew cyclic (of all orders).

Proof. Since $\theta_1(V) \subseteq V$, it holds that $\theta_r(V) = V$, for all $r \geq 0$. Hence, if we fix two integers $r, s \geq 0$, we have that $\sigma_{r,n}(V) \subseteq V$ if, and only if, $\sigma_{s,n}(V) \subseteq V$, and the first statement follows.

For the second statement, assume that C is q^r -cyclic. It holds that

$$\sigma_{r,n}(C^*) = \sum_{i=0}^{m-1} \sigma_{r,n}(C^{[i]}) = \sum_{i=0}^{m-1} \sigma_{r,n}(C)^{[i]} \subseteq \sum_{i=0}^{m-1} C^{[i]} = C^*,$$

and similarly for C^0 , and we are done. \square

By the discussion after [13, Lemma 10], it follows that $l_R(C)$ is equal to the k -th generalized rank weight of C [10, Definition 2], for $k = \dim(C)$, which is the dimension of C^* by [9, Corollary 17]. That is,

$$l_R(C) = d_{R,k}(C) = \dim(C^*). \quad (1)$$

We may establish now the following relations between the different types of lengths:

Proposition 1. *For any integers $r, s \geq 0$, a linear q^s -cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ and an element $a \in \mathbb{F}_q^*$, it holds that*

1. $l_R(C) \leq l_{Sk,s}(C) \leq l_{Sh,a,r}(C)$.
2. $l_{Sh,1,r}(C) \leq l_P(C)$.
3. $l_R(C) = l_R(C^*)$, $l_{Sh,a,r}(C) = l_{Sh,a,r}(C^*)$ and $l_P(C) = l_P(C^*)$.
4. $l_{Sk,r}(C) \geq l_{Sk,r}(C^*) = l_R(C)$.

Proof. In item 1, the first inequality is trivial and the second one follows from Remark 2.

To prove item 2, we see that puncturing in the first $l_P(C)$ coordinates gives a rank equivalence from C^* to a linear Galois closed subspace of $\mathbb{F}_{q^m}^{l_P(C)}$ that commutes with $\sigma_{r,n}$, and the inequality follows.

We now prove item 3. First, $l_R(C) = \dim(C^*) = \dim(C^{**}) = l_R(C^*)$ by (1). Now, if ϕ is a rank equivalence between C and a skew cyclic code C' such that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$, then ϕ preserves Galois closures, and hence C^* is rank equivalent to C'^* by ϕ . It follows that $l_{Sh,a,r}(C) \geq l_{Sh,a,r}(C^*)$, being the reversed inequality obvious. On the other hand, it follows from the definitions that $l_P(C) = l_P(C^*)$.

Finally, item 4 is proven in the same way as the fact that $l_{Sh,a,r}(C) \geq l_{Sh,a,r}(C^*)$. The fact that $l_{Sk,r}(C^*) = l_R(C^*)$ follows from the definitions. \square

Corollary 1. *For any linear skew cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ and any $i = R, (Sk, r), (Sh, a, r), P$, we have the following Singleton-type bounds:*

$$d_R(C) \leq l_i(C) - k + 1,$$

where d_R denotes the minimum rank distance.

Proof. The case $i = R$ follows from the classical Singleton bound [5] and the fact that there exists a linear code of length $l_R(C)$ that is rank equivalent to C . The rest of the bounds follow from this case and the previous proposition. \square

Remark 3. If we denote by $d_{R,r}(C)$ the r -th generalized rank weight of a linear skew cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ (see [10, Definition 2]), for $1 \leq r \leq k$, then using that $l_R(C) = d_{R,k}(C)$, the monotonicity of generalized rank weights [10, Lemma 4] and Proposition 1, we obtain the following generalized Singleton-type bounds:

$$d_{R,r}(C) \leq l_i(C) - k + r.$$

4 Using the conventional-polynomial representation of Galois closures

It is well-known [8, Chapter 4] that a linear cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ can be represented as an ideal $C(x)$ in the quotient ring $\mathbb{F}_{q^m}[x]/(x^n - 1)$, and it has unique polynomials $g(x), h(x) \in \mathbb{F}_{q^m}[x]$, called generator and check polynomials, respectively, such that $g(x)$ is monic and of minimal degree among those with residue class in $C(x)$, and $g(x)h(x) = x^n - 1$. Moreover, $g(x)$ generates $C(x)$.

There are two more descriptions of linear cyclic codes. If $g(x)$ and $h(x)$ are coprime (which holds if q and n are coprime), then there exists a unique idempotent polynomial $e(x) \in C(x)$ (that is, $e(x)^2 = e(x)$ in $\mathbb{F}_{q^m}[x]/(x^n - 1)$) that generates $C(x)$ [8, Theorem 4.3.2].

On the other hand, for a given polynomial $f(x) \in \mathbb{F}_{q^m}[x]$, let $Z(f(x))$ denote the set of its roots in its splitting field. If q and n are coprime, then we may associate C with the root set $Z(g(x))$. This gives a bijective correspondence between linear cyclic codes in $\mathbb{F}_{q^m}^n$ and root sets of divisors of $x^n - 1$ [8, Section 4.4].

In this section we will focus on this conventional-polynomial representation of linear cyclic codes (in contrast with the linearized-polynomial representation in the following sections), which may be used for the Galois closure of any linear skew cyclic code by Lemma 2.

Observe that the r -th Frobenius map θ_r induces a ring automorphism $\theta_r : \mathbb{F}_{q^m}[x] \longrightarrow \mathbb{F}_{q^m}[x]$ given by

$$\theta_r(f_0 + f_1x + \cdots + f_dx^d) = f_0^{[r]} + f_1^{[r]}x + \cdots + f_d^{[r]}x^d, \quad (2)$$

for all $f_0 + f_1x + \cdots + f_dx^d \in \mathbb{F}_{q^m}[x]$. Since $\theta_r(x^n - 1) = x^n - 1$, it induces a ring automorphism of the quotient ring $\mathbb{F}_{q^m}[x]/(x^n - 1)$.

Recall from [8, Exercise 243] that, again if $g(x)$ and $h(x)$ are coprime, then there exists a unique linear cyclic code C^c such that $C \oplus C^c = \mathbb{F}_{q^m}^n$, called the cyclic complementary code of C . Its generator and check polynomials are $h(x)$ and $g(x)$, respectively, its idempotent generator is $1 - e(x)$ and its root set is $Z(h(x)) = Z(x^n - 1) \setminus Z(g(x))$.

We have the following expected characterizations:

Lemma 3. *Given a linear cyclic code $C \subseteq \mathbb{F}_{q^m}^n$ as in the beginning of this section, the following are equivalent:*

1. C is Galois closed.
2. $g(x) \in \mathbb{F}_q[x]$.
3. $h(x) \in \mathbb{F}_q[x]$.
4. (If $g(x)$ and $h(x)$ are coprime) $e(x) \in \mathbb{F}_q[x]$.
5. (If q and n are coprime) $Z(g(x))^q = Z(g(x))$.
6. (If $g(x)$ and $h(x)$ are coprime) C^c is Galois closed.

Proof. It is enough to note the following:

1. $\theta_1(C)$ has $\theta_1(g(x))$ as generator polynomial, since it generates $\theta_1(C)(x)$ and θ_1 preserves monic polynomials and degrees. Hence the equivalence between items 1 and 2 follows.
2. $\theta_1(C)$ has $\theta_1(h(x))$ as check polynomial, by the fact that $x^n - 1 = \theta_1(x^n - 1) = \theta_1(g(x))\theta_1(h(x))$ and the previous item in this proof. Hence the equivalence between items 1 and 3 follows.
3. If $g(x)$ and $h(x)$ are coprime, then $\theta_1(C)$ has $\theta_1(e(x))$ as idempotent generator, since $\theta_1(e(x))$ is again idempotent, generates $\theta_1(C)(x)$ and the idempotent generator is unique [8, Theorem 4.3.2]. Hence the equivalence between items 1 and 4 follows.
4. If q and n are coprime, then $\theta_1(C)$ corresponds to the root set $Z(g(x))^q$, since $Z(\theta_1(g(x))) = Z(g(x))^q$. Hence the equivalence between items 1 and 5 follows.

Finally, the equivalence between items 1 and 6 follows from the fact that $h(x)$ and $g(x)$ are the generator and check polynomials of C^c , respectively. \square

We now characterize rank equivalences that commute with the q^r -shifting operators in terms of generator matrices. For a matrix X over \mathbb{F}_{q^m} with n columns, we define $\sigma_{r,n}(X)$ as the matrix such that its i -th row is the q^r -shifted i -th row of X .

Recall from [17, Lemma 1] that linear Galois closed spaces are those with a basis of vectors in \mathbb{F}_q^n , that is, a generator matrix with coefficients in \mathbb{F}_q .

Proposition 2. *For linear cyclic Galois closed spaces $V \subseteq \mathbb{F}_{q^m}^n$ and $V' \subseteq \mathbb{F}_{q^m}^{n'}$, and a rank equivalence $\phi : V \rightarrow V'$, where we define β and A as in Lemma 1, the following are equivalent for a given $a \in \mathbb{F}_q^*$ and $r \geq 0$:*

1. $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$.
2. If G is a generator matrix of V , then $\sigma_{r,n}(G)A = a\beta^{[r]-1}\theta_r(G)s_{n'}(A)$.

In particular, choosing G with coefficients in \mathbb{F}_q , the second item reads $s_n(G)A = a\beta^{[r]-1}Gs_{n'}(A)$. Therefore, if any of the previous items hold, then $\beta^{[r]-1} = b \in \mathbb{F}_q^*$.

Proof. For any vector $\mathbf{c} \in V$, it is a straightforward computation to verify that condition 1 is equivalent to

$$\sigma_{r,n}(\mathbf{c})A = a\beta^{[r]-1}\theta_r(\mathbf{c})s_{n'}(A).$$

Therefore, the equivalence between items 1 and 2 follows from the linearity of ϕ and the semi-linearity of the q^r -shifting operators. \square

Remark 4. If $V = \mathbb{F}_{q^m}^n$, then item 2 means that $s_{n'}(\mathbf{a}_i) = a^{-1}\beta^{1-[r]}\mathbf{a}_{i+1}$, where indices i are taken modulo n , and \mathbf{a}_i denotes the i -th row in A .

On the other hand, if $V' = \mathbb{F}_{q^m}^{n'}$, then item 2 means that $s_n(\mathbf{a}'_i) = a\beta^{[r]-1}\mathbf{a}'_{i+1}$, where \mathbf{a}'_i is the i -th row of a matrix A' with $AA' = I$ (observe that $n' \leq n$ in this case).

On the other hand, the check polynomials of V and V' can be easily used to see whether there exists such a rank equivalence between them, which is the first main result of this section:

Theorem 1. Let $V \subseteq \mathbb{F}_{q^m}^n$ and $V' \subseteq \mathbb{F}_{q^m}^{n'}$ be linear cyclic Galois closed spaces with the same dimension k and check polynomials $h(x)$ and $h'(x)$, respectively. Given $a \in \mathbb{F}_q^*$, an integer $r \geq 0$ and $\beta \in \mathbb{F}_{q^m}^*$ such that $\beta^{[r]} = b\beta$, for some $b \in \mathbb{F}_q^*$, the following are equivalent:

1. There exists a rank equivalence $\phi : V \longrightarrow V'$ such that $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$ and β is as in Lemma 1.
2. $(ab)^k h'(x) = h(abx)$.
3. (If q and n are coprime) $abZ(h'(x)) = Z(h(x))$.

Proof. It is obvious that items 2 and 3 are equivalent. We next prove the equivalence between items 1 and 2:

We first prove that item 1 implies item 2. Let $h(x) = h_0 + h_1x + \dots + h_kx^k$. Assume that there exists a rank equivalence $\phi : V \longrightarrow V'$ satisfying item 1. Let $g(x) = g_0 + g_1x + \dots + g_{n-k}x^{n-k}$ be the generator polynomial of V , and let $\mathbf{g} = (g_0, g_1, \dots, g_{n-k}, 0, \dots, 0) \in \mathbb{F}_q^n$. Define $f(x) = f_0 + f_1x + \dots + f_{n-1}x^{n-1} \in \mathbb{F}_{q^m}[x]$ such that $\mathbf{f} = (f_0, f_1, \dots, f_{n-1}) = \phi(\mathbf{g})$. By Lemma 1, we have that $f(x) = \beta\tilde{f}(x)$, for some $\tilde{f}(x) \in \mathbb{F}_q[x]$.

It holds that $a^i\sigma_{r,n'}^i(\mathbf{f}) = \phi(\sigma_{r,n}^i(\mathbf{g}))$, for $i = 0, 1, 2, \dots, k$. In polynomial representation, we have that $\sigma_{r,n}^i(\mathbf{g})$ corresponds to $x^i g(x)$, and $x^k g(x) = \sum_{i=0}^{k-1} -h_i x^i g(x)$. On the other hand, $\sigma_{r,n'}^i(\mathbf{f})$ corresponds to $x^i \theta_r^i(f(x)) = x^i \beta^{[ir]} \tilde{f}(x) = x^i b^i \beta \tilde{f}(x)$. Hence it follows that $x^k a^k b^k \tilde{f}(x) = \sum_{i=0}^{k-1} -h_i a^i b^i x^i \tilde{f}(x)$. In other words, $h(abx)\tilde{f}(x) = 0$.

On the other hand, the vectors $\sigma_{r,n'}^i(\mathbf{f}) = a^{-i}\phi(\sigma_{r,n}^i(\mathbf{g}))$, $i = 0, 1, \dots, k-1$, constitute a basis of V' , which implies that $\tilde{f}(x), x\tilde{f}(x), \dots, x^{k-1}\tilde{f}(x)$ constitute a basis of $V'(x)$. Hence, $\tilde{f}(x)$ generates the ideal $V'(x)$. Since $h(abx)\tilde{f}(x) = 0$, we conclude by degrees that $h(abx) = (ab)^k h'(x)$, and we are done.

Now we prove that item 2 implies item 1. Let $\mathbf{g}' = (g'_0, g'_1, \dots, g'_{n'-k}, 0, \dots, 0) \in \mathbb{F}_{q^m}^{n'}$ by such that $g'(x) = g'_0 + g'_1x + \dots + g'_{n'-k}x^{n'-k}$ is the generator polynomial of V' . We just need to define ϕ by the formula

$$\phi(\sigma_{r,n}^i(\mathbf{g})) = a^i \sigma_{r,n'}^i(\beta \mathbf{g}') = (a^i b^i) \beta \sigma_{r,n'}^i(\mathbf{g}'), \quad (3)$$

for $i = 0, 1, 2, \dots, k-1$, which defines a rank equivalence between V and V' by Lemma 1, and see that this formula also holds for $i = k$. If that happens, then the equality $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$ holds on a basis of V and then it holds on all V .

To see that Equation (3) also holds for $i = k$, we may argue as in the converse implication by using again that $(ab)^k h'(x) = h(abx)$. \square

Observe from the previous proof that each of such equivalences is constructed by Equation (3) using a polynomial $f(x) \in V'(x)$ with coefficients in \mathbb{F}_q and such that $f(x), xf(x), \dots, x^{k-1}f(x)$ generate $V'(x)$ as a vector space.

Taking $a = b = 1$, we obtain the following particular case:

Corollary 2. *Let V, V' and $h(x), h'(x)$ be as in the previous theorem. The following are equivalent:*

1. *There exists a matrix $A \in \mathbb{F}_q^{n \times n'}$, mapping V to V' , such that $\phi : V \rightarrow V'$ given by $\phi(\mathbf{c}) = \mathbf{c}A$, $\mathbf{c} \in V$, satisfies $\sigma_{r,n'} \circ \phi = \phi \circ \sigma_{r,n}$.*
2. *$h'(x) = h(x)$.*
3. *(If q and n are coprime) $Z(h'(x)) = Z(h(x))$.*

On the other hand, given a polynomial $f(x) \in \mathbb{F}_{q^m}[x]$, we define its order as the minimum positive integer e such that $f(x)$ divides $x^e - 1$ (in $\mathbb{F}_{q^m}[x]$), and denote it by $\text{ord}(f(x))$. In general, for $a \in \mathbb{F}_q$, we define the a -order of $f(x)$ as the minimum positive integer e such that $f(x)$ divides $x^e - a^e$ (in $\mathbb{F}_{q^m}[x]$), if one such e exists, and denote it by $\text{ord}_a(f(x))$. If no such e exists, we define $\text{ord}_a(f(x)) = \infty$.

We may now prove the second main result of this section:

Theorem 2. *For an integer $s \geq 0$ and a linear q^s -cyclic code $C \subseteq \mathbb{F}_{q^m}^n$, where $h^0(x)$ is the check polynomial of C^* , it holds that*

1. $l_R(C) = \deg(h^0(x))$.
2. $l_{Sh,1,0}(C) = l_P(C) = \text{ord}(h^0(x)) \leq n$.
3. *More generally, if $a \in \mathbb{F}_q^*$, then $e = l_{Sh,a,0}(C) = \text{ord}_a(h^0(x))$ and e is an a^e -period of C .*
4. *More generally, if $a \in \mathbb{F}_q^*$ and $r \geq 0$, then*

$$l_{Sh,a,r}(C) = \min\{\text{ord}_{ab}(h^0(x)) \mid b \in \mathbb{F}_q^*, \beta \in \mathbb{F}_{q^m}^*, \beta^{[r]} = b\beta\}.$$

In particular, $l_R(C) = l_{Sk,s}(C) = l_{Sh,1,r}(C) = l_P(C)$ if, and only if, $\deg(h^0(x)) = \text{ord}(h^0(x))$, which holds if, and only if, $h^0(x) = x^e - 1$, for some positive integer e .

Proof. First of all, we have seen that $l_R(C) = \dim(C^*)$, and this dimension is $\deg(h^0(x))$. Hence item 1 follows.

Now, the equality $l_{Sh,1,0}(C) = \text{ord}(h^0(x))$ in item 2 follows from item 3 by choosing $a = 1$, and it is straightforward to see that $\text{ord}(h^0(x))$ is equal to $l_P(C)$.

Item 3 follows now from item 4, since $\beta^{[0]} = \beta$, for all $\beta \in \mathbb{F}_{q^m}$. Moreover, since $x^e f(x) = a^e f(x)$, for all $f(x) \in C(x)$, we see that e is an a^e -period of C .

Next we prove item 4. Assume that there exists a rank equivalence $\phi : C^* \longrightarrow V'$, where V' is a linear cyclic Galois closed space of length e and $a(\sigma_{r,n'} \circ \phi) = \phi \circ \sigma_{r,n}$. By the previous theorem, the check polynomial of V' is $(ab)^{-k} h^0(abx)$, $k = \dim(C^*)$, with notation as in the previous theorem. Hence, we see that $h^0(x)$ divides $x^e - (ab)^e$, since $h^0(abx)$ divides $x^e - 1$.

Conversely, if $h^0(x)$ divides $x^e - (ab)^e$, we may define the linear cyclic Galois closed space $V' \subseteq \mathbb{F}_{q^m}^e$ with check polynomial $h'(x) = (ab)^{-k} h^0(abx)$, which divides $x^e - 1$. Then there exists a rank equivalence $\phi : C^* \longrightarrow V'$ as before by the previous theorem.

Therefore, choosing the elements b and β that minimize the number e , we see that $l_{Sh,a,r}(C) = \text{ord}_{ab}(h^0(x))$, and item 4 follows.

Finally, by Proposition 1, we conclude that $l_R(C) = l_{Sk,s}(C) = l_{Sh,1,r}(C) = l_P(C)$ if, and only if, $\deg(h^0(x)) = \text{ord}(h^0(x))$. It is straightforward to see that this is equivalent to $h^0(x) = x^e - 1$, $e = \text{ord}(h^0(x))$. \square

Remark 5. We see from the previous theorem that there are three instances of $h^0(x)$ that give an easy description of C and where $l_R(C)$ is attained by a linear skew cyclic code:

1. $h^0(x) = x^e - 1$, for some positive integer $e \leq n$. This case has two subcases:
 - (a) $e = n$, which corresponds to the case where C is not rank degenerate.
 - (b) $e < n$, in which case C is rank degenerate in a special way: e divides n and C is constructed by repeating n/e times a linear skew cyclic code $C' \subseteq \mathbb{F}_{q^m}^e$ that is not rank degenerate.
2. There exists an $a \in \mathbb{F}_q^*$ and a positive integer $e < n$ with $h^0(x) = x^e - a^e$. In this case, e divides n , $a^n = 1$ and again C is constructed by repeating n/e times a linear skew cyclic code $C' \subseteq \mathbb{F}_{q^m}^e$ that is not rank degenerate.

Observe that $a^n = 1$ since $x^e - a^e$ divides $x^n - 1$. Then we see that $a^e((a^{-1}x)^e - 1)$ divides $(a^{-1}x)^n - 1 = x^n - 1$, hence $x^e - 1$ divides $x^n - 1$, which implies that e divides n .

In the next sections we will give results on C in terms of its structure, and relate it to the structure of C^* and C^0 .

5 Cyclic codes, conventional polynomials and root sets

Given a polynomial $f(x) \in \mathbb{F}_{q^m}[x]$, we define the following polynomials, where divisibility is considered in $\mathbb{F}_{q^m}[x]$:

$$f^*(x) = \gcd(f(x), \theta_1(f(x)), \dots, \theta_{m-1}(f(x))), \quad (4)$$

$$f^0(x) = \text{lcm}(f(x), \theta_1(f(x)), \dots, \theta_{m-1}(f(x))), \quad (5)$$

$$f^\perp(x) = x^{\deg(f(x))} f(x^{-1}) / f(0), \quad (6)$$

assuming $f(0) \neq 0$ in the last equation. We have the following:

Lemma 4. *For any polynomial $f(x) \in \mathbb{F}_{q^m}[x]$, it holds that $f^*(x), f^0(x) \in \mathbb{F}_q[x]$.*

Proof. Since θ_1 leaves the set $\{f(x), \theta_1(f(x)), \dots, \theta_{m-1}(f(x))\}$ invariant and is a ring automorphism, it holds that $\theta_1(f^*(x)) = f^*(x)$ and $\theta_1(f^0(x)) = f^0(x)$, which mean that both lie in $\mathbb{F}_q[x]$. \square

Now fix a linear cyclic code $C \subseteq \mathbb{F}_{q^m}^n$, whose generator and check polynomials are $g(x)$ and $h(x)$, respectively. It is well-known that $h^\perp(x)$ and $g^\perp(x)$ are the generator and check polynomials of C^\perp , respectively [8, Theorem 4.2.7]. The following proposition explains the previous notation:

Proposition 3. *The generator and check polynomials of C^* are $g^*(x)$ and $h^0(x)$, respectively, and the generator and check polynomials of C^0 are $g^0(x)$ and $h^*(x)$, respectively. In particular,*

$$\begin{aligned} (g^*)^\perp(x) &= (g^\perp)^*(x), & (g^0)^\perp(x) &= (g^\perp)^0(x), \\ (h^*)^\perp(x) &= (h^\perp)^*(x), & \text{and } (h^0)^\perp(x) &= (h^\perp)^0(x). \end{aligned}$$

Proof. Taking ideals, it holds that $C(x) = \sum_{i=0}^{m-1} C^{[i]}(x)$, and $C^{[i]}$ has $\theta_i(g(x))$ as generator polynomial. It is well-known that the generator polynomial of the sum of cyclic codes is the greatest common divisor of their generator polynomials [8, Theorem 4.3.7].

Hence the polynomial $g^*(x)$ is the generator polynomial of C^* . Similarly $g^0(x)$ is the generator polynomial of C^0 , using now that the generator polynomial of the intersection of cyclic codes is the least common multiple of their generator polynomials [8, Theorem 4.3.7].

On the other hand, we have that $\theta_i(g(x))\theta_i(h(x)) = \theta_i(x^n - 1) = x^n - 1$, for $i = 0, 1, 2, \dots, m-1$. Hence the greatest common divisor of the polynomials $\theta_i(g(x))$ and the least common multiple of the polynomials $\theta_i(h(x))$ satisfy the same. That is, $g^*(x)h^0(x) = x^n - 1$, and $h^0(x)$ is the check polynomial of C^* . Similarly for C^0 .

Finally, since $g^\perp(x)$ is the check polynomial of C^\perp , it follows that $(g^\perp)^*(x)$ is the check polynomial of $(C^\perp)^0$. On the other hand, since $g^*(x)$ is the generator polynomial of C^* , it holds that $(g^*)^\perp(x)$ is the check polynomial of $(C^*)^\perp$. Since $(C^\perp)^0 = (C^*)^\perp$, it follows that $(g^*)^\perp(x) = (g^\perp)^*(x)$. The remaining equalities are proven in the same way. \square

On the other hand, we have the following relations of idempotent generators and cyclic complementaries.

Proposition 4. *Assume that $g(x)$ and $h(x)$ are coprime and $e(x)$ is the idempotent generator of C . Then C^* and C^0 have $1 - \prod_{i=0}^{m-1} (1 - \theta_i(e(x)))$ and $\prod_{i=0}^{m-1} \theta_i(e(x))$ as idempotent generators, respectively. Moreover it holds that*

$$(C^c)^* = (C^0)^c \quad \text{and} \quad (C^c)^0 = (C^*)^c.$$

Proof. First, the idempotent generator of the intersection of cyclic codes is the product of their idempotent generators [8, Theorem 4.3.7], hence $\prod_{i=0}^{m-1} \theta_i(e(x))$ is the idempotent generator of C^0 .

On the other hand, C^c has $h(x)$ as generator polynomial, thus $(C^c)^*$ has $h^*(x)$ as generator polynomial by the previous proposition. Moreover, C^0 has $h^*(x)$ as check polynomial, also by the previous proposition. Therefore $(C^c)^* = (C^0)^c$. Similarly we may prove that $(C^c)^0 = (C^*)^c$.

Finally, It holds that $\prod_{i=0}^{m-1} (1 - \theta_i(e(x)))$ is the idempotent generator of $(C^c)^0$ by the first part of this proof. Using that $(C^c)^0 = (C^*)^c$, we see that $1 - \prod_{i=0}^{m-1} (1 - \theta_i(e(x)))$ is the idempotent generator of C^* . \square

In addition, we may easily see that C^c and C^\perp are rank equivalent:

Proposition 5. *Assume that $g(x)$ and $h(x)$ are coprime. Then C^c and C^\perp are rank equivalent.*

Proof. There exists a permutation of indices that maps C^c to C^\perp by [8, Theorem 4.4.9], which obviously defines a rank equivalences between them. \square

We will now relate C , C^* and C^0 by means of the defining root set of C . We will relate $l_R(C^\perp)$ with the parameter $\eta_q(C)$ introduced in [4], which will allow us to easily derive the main results in that paper.

If q and n are coprime, let $m' \geq m$ be such that $\mathbb{F}_{q^{m'}}$ is the splitting field of $g(x)$. Let $\alpha_1, \alpha_2, \dots, \alpha_{n-k} \in \mathbb{F}_{q^{m'}}$ be the simple roots of $g(x)$, and assume that they are ordered in the following way: there exist $1 = m_0 < m_1 < m_2 < \dots < m_t = n - k + 1$ such that $\alpha_{m_i}, \alpha_{m_i+1}, \dots, \alpha_{m_{i+1}-1}$ are roots of the minimal polynomial $\mu_i(x) \in \mathbb{F}_q[x]$ of α_{m_i} over \mathbb{F}_q , for $i = 0, 1, \dots, t-1$.

Definition 3 ([4, Definition 3, Definition 4]). With notation as in the previous paragraph, we define

$$\mu_q(g(x)) = \prod_{i=0}^{t-1} \mu_i(x) \in \mathbb{F}_q[x] \quad \text{and} \quad \eta_q(C) = \deg(\mu_q(g(x))).$$

We have the following relations, which in particular compute the root set corresponding to C^* and C^0 :

Proposition 6. *If q and n are coprime, then*

1. $\mu_q(g(x)) = g^0(x)$.
2. $Z(g^0(x)) = \bigcup_{i=0}^{m-1} Z(g(x))^{[i]}$ and $Z(g^*(x)) = \bigcap_{i=0}^{m-1} Z(g(x))^{[i]}$.
3. $\eta_q(C) = \deg(g^0(x)) = \dim((C^\perp)^*)$ and $\deg(g^*(x)) = \dim((C^\perp)^0)$.

Analogous identities hold replacing $g(x)$, $g^*(x)$ and $g^0(x)$ by $h(x)$, $h^*(x)$ and $h^0(x)$, respectively.

Proof. First, $g(x)$ divides $\mu_q(g(x))$ in $\mathbb{F}_{q^{m'}}[x]$ by looking at their roots. By the same argument as in Lemma 3, we see that $g(x)$ divides $\mu_q(g(x))$ in $\mathbb{F}_{q^m}[x]$.

Fix a positive integer r . Since θ_r is a ring isomorphism, we see that $\theta_r(g(x))$ also divides $\theta_r(\mu_q(g(x))) = \mu_q(g(x))$ in $\mathbb{F}_{q^m}[x]$. Hence $\mu_q(g(x))$ is divisible by the least common multiple of the polynomials $\theta_r(g(x))$, $r = 0, 1, 2, \dots, m-1$.

Finally, since the Galois group of the extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^{m'}}$ is constituted by the maps θ_r , we see that the previous least common multiple vanishes at the roots of the polynomials $\mu_i(x)$, for $i = 0, 1, \dots, t-1$. Hence $\mu_q(g(x)) = \text{lcm}(g(x), \theta_1(g(x)), \dots, \theta_{m-1}(g(x))) = g^0(x)$ and item 1 follows.

By the same discussion, since $Z(\theta_i(g(x))) = Z(g(x))^{[i]}$, we have that $Z(g^0(x)) = \bigcup_{i=0}^{m-1} Z(g(x))^{[i]}$. On the other hand, denoting $Z = Z(x^n - 1)$ and using that $g^*(x)h^0(x) = g(x)h(x) = x^n - 1$, we have that

$$Z(g^*(x)) = Z \setminus Z(h^0(x)) = Z \setminus \left(\bigcup_{i=0}^{m-1} Z(h(x))^{[i]} \right) = \bigcap_{i=0}^{m-1} (Z \setminus Z(h(x))^{[i]}) = \bigcap_{i=0}^{m-1} Z(g(x))^{[i]},$$

and item 2 follows. Item 3 follows from item 1 and Proposition 3. \square

Remark 6. Hence C^\perp is rank degenerate if, and only if, $\eta_q(C) < n$, which by the duality theorem for generalized rank weights [3, Theorem] is equivalent to $d_R(C) = 1$ (see [3] for more details). Hence [4, Proposition 2] and [4, Proposition 3] follow. We have actually proven that

$$\eta_q(C) = l_R(C^\perp), \tag{7}$$

which combined with the same duality theorem also implies [4, Proposition 5]. Moreover, together with Corollary 1 we obtain [4, Proposition 6].

We may now state the main result of this section, which computes lengths of cyclic codes in terms of their intrinsic structure:

Theorem 3. *It holds that*

$$\begin{aligned} l_R(C) &= n - \deg(\gcd(g(x), \theta_1(g(x)), \dots, \theta_{m-1}(g(x)))) \\ &= \deg(\text{lcm}(h(x), \theta_1(h(x)), \dots, \theta_{m-1}(h(x)))), \end{aligned}$$

and if q and n are coprime, then

$$l_R(C) = \eta_q(C^\perp) = n - \# \left(\bigcap_{i=0}^{m-1} Z(g(x))^{[i]} \right) = \# \left(\bigcup_{i=0}^{m-1} Z(h(x))^{[i]} \right).$$

On the other hand, for $a \in \mathbb{F}_q^*$, it holds that

$$\begin{aligned} l_{Sh,a,0}(C) &= \text{ord}_a(h^0(x)) = \text{ord}_a(h(x)) = \text{ord}_a(\mu_q(h(x))) \\ &= \min\{e \mid \alpha^e = a^e, \forall \alpha \in Z(h(x))\}. \end{aligned}$$

Proof. The first two equalities follow from Theorem 2, item 1, and Proposition 3. If q and n are coprime, then the next three equalities follow from the same results as before together with Proposition 6 and Equation (7). Finally, the last four equalities follow from the same results as before together with Theorem 2, items 2 and 3. \square

The following characterizations of rank degenerate cyclic codes follow:

Corollary 3. *The following conditions are equivalent:*

1. C is rank degenerate. That is, $l_R(C) < n$.
2. $\gcd(g(x), \theta_1(g(x)), \dots, \theta_{m-1}(g(x))) \neq 1$.
3. $\text{lcm}(h(x), \theta_1(h(x)), \dots, \theta_{m-1}(h(x))) \neq x^n - 1$.
4. (If $g(x)$ and $h(x)$ are coprime) $\prod_{i=0}^{m-1} (1 - \theta_i(e(x))) = 0$ in $\mathbb{F}_{q^m}[x]/(x^n - 1)$, where $e(x)$ is the idempotent generator of C .
5. (If q and n are coprime) $\eta_q(C^\perp) < n$.
6. (If q and n are coprime) $\bigcap_{i=0}^{m-1} Z(g(x))^{[i]} \neq \emptyset$.
7. (If q and n are coprime) $\bigcup_{i=0}^{m-1} Z(h(x))^{[i]} \subsetneq Z(x^n - 1)$.
8. $g(x)$ is divisible by some non-constant polynomial $f(x) \in \mathbb{F}_q[x]$ (in $\mathbb{F}_{q^m}[x]$).
9. $h(x)$ divides some polynomial $f(x) \in \mathbb{F}_q[x]$ (in $\mathbb{F}_{q^m}[x]$) of degree less than n .

6 Skew cyclic codes, linearized polynomials and root spaces

In this section we will fix a positive integer r and assume that m divides rn , and will use the linearized-polynomial description of skew cyclic codes given in [1, 5, 6, 12] to give similar characterizations of lengths and rank degenerateness as in the previous section for general skew cyclic codes. By the discussion after [12, Remark 2], assuming that m divides rn does not leave any skew cyclic code out of study regarding the lengths $l_i(C)$.

Denote by $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ the ring of q^r -linearized polynomials over \mathbb{F}_{q^m} (see [5, 14, 15] or [11, Chapter 3]), that is, polynomials of the form

$$F(x) = F_0x + F_1x^{[r]} + F_2x^{[2r]} + \cdots + F_dx^{[dr]},$$

where $F_0, F_1, F_2, \dots, F_d \in \mathbb{F}_{q^m}[x]$, and where we consider composition of maps \otimes as product. We also define the q^r -degree of $F(x)$ as $\deg_{q^r}(F(x)) = d$ if $F_d \neq 0$.

Recall that q^r -linearized polynomials over \mathbb{F}_{q^m} define \mathbb{F}_{q^r} -linear maps between field extensions of \mathbb{F}_{q^r} and their compositions as such define again q^r -linearized polynomials over \mathbb{F}_{q^m} . This ring constitutes an Euclidean domain on the right and on the left [5, 14, 15], but we will always consider divisibility on the right. We will also use the term “conventional” to refer to the usual product and divisibility of polynomials.

Since m divides rn , $x^{[rn]} - x$ commutes with every other q^r -linearized polynomial over \mathbb{F}_{q^m} and the left ideal $(x^{[rn]} - x)$ is two-sided. Thus, we may consider the ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, which is isomorphic to $\mathbb{F}_{q^m}^n$ as a vector space.

Linear q^r -cyclic codes correspond to left ideals in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$ [1, 5, 6]. Fix one $C \subseteq \mathbb{F}_{q^m}^n$. It has unique generator polynomial $G(x)$ and check polynomial $H(x)$ with the same properties as in the usual case [1, 6, 12]: $G(x)$ is of minimal degree and monic, and $x^{[rn]} - x = G(x) \otimes H(x) = H(x) \otimes G(x)$.

For a given $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, we will also write $F = F(x) + (x^{[rn]} - x)$, the residue class of $F(x)$ modulo $x^{[rn]} - x$. Recall that, since q^r -linearized polynomials induce \mathbb{F}_{q^r} -linear maps, their root sets are \mathbb{F}_{q^r} -linear vector spaces. We may denote by $Z(F)$ the \mathbb{F}_{q^r} -linear space of zeroes in $\mathbb{F}_{q^{rn}}$ of $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$. This definition is consistent, since two q^r -polynomials $F_1(x)$ and $F_2(x)$ have the same roots in \mathbb{F}_{q^r} if $F_1(x) - F_2(x) \in (x^{[rn]} - x)$.

On the other hand, the s -th Frobenius map θ_s defines also a ring automorphism $\theta_s : \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x] \rightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ using the same formula as in the conventional case (2) and induces a ring automorphism of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(x^{[rn]} - x)$, since $\theta_r(x^{[rn]} - x) = x^{[rn]} - x$.

In this section we will consider the q^r -cyclic structure of linear Galois closed spaces. However, describing generator and check polynomials of C^\perp , C^* and C^0 is not as straightforward as in the conventional case. Given a q^r -polynomial $F(x) = F_0x + F_1x^{[r]} + \cdots + F_dx^{[rd]} \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ that divides $x^{[rn]} - x$, with $F_d \neq 0$, we define:

$$F^\perp(x) = \left(\frac{F_d}{F_0^{[dr]}} \right) x + \left(\frac{F_{d-1}^{[r]}}{F_0^{[dr]}} \right) x^{[r]} + \cdots + \left(\frac{F_0^{[dr]}}{F_0^{[dr]}} \right) x^{[dr]}, \quad (8)$$

$$F^\top(x) = \left(\frac{F_d}{F_0} \right)^{[(n-d)r]} x + \left(\frac{F_{d-1}}{F_0} \right)^{[(n-d+1)r]} x^{[r]} + \cdots + \left(\frac{F_0}{F_0} \right)^{[nr]} x^{[dr]}, \quad (9)$$

$$F^*(x) = \gcd(F(x), \theta_1(F(x)), \dots, \theta_{m-1}(F(x))), \quad (10)$$

$$F^0(x) = \text{lcm}(F(x), \theta_1(F(x)), \dots, \theta_{m-1}(F(x))), \quad (11)$$

$$F_*(x) = \gcd(F(x)^\perp, \theta_1(F(x))^\perp, \dots, \theta_{m-1}(F(x))^\perp)^\top, \quad (12)$$

$$F_0(x) = \text{lcm}(F(x)^\perp, \theta_1(F(x))^\perp, \dots, \theta_{m-1}(F(x))^\perp)^\top. \quad (13)$$

As in the previous section, we have the following:

Lemma 5. *For any q^r -polynomial $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, it holds that $F^*(x)$, $F^0(x)$, $F_*(x)$, $F_0(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$.*

Proof. Since θ_1 leaves the set $\{F(x), \theta_1(F(x)), \dots, \theta_{m-1}(F(x))\}$ invariant and is a ring automorphism, it holds that $\theta_1(F^*(x)) = F^*(x)$ and $\theta_1(F^0(x)) = F^0(x)$. Observing that $\theta_1(F^\perp(x)) = \theta_1(F(x))^\perp$ and $\theta_1(F^\top(x)) = \theta_1(F(x))^\top$, we see that $\theta_1(F_*(x)) = F_*(x)$ and $\theta_1(F_0(x)) = F_0(x)$. Hence the result follows. \square

Remark 7. *Observe that taking $r = m$, we obtain a q^m -linearized description of cyclic codes and n may be arbitrary. Observe that $\mathcal{L}_{q^m}\mathbb{F}_{q^m}[x]$ is commutative and naturally isomorphic to $\mathbb{F}_{q^m}[x]$ by the map given in [11, Definition 3.58]:*

$$L(f_0 + f_1x + \dots + f_dx^d) = f_0x + f_1x^{[m]} + \dots + f_dx^{[md]}. \quad (14)$$

In particular, $L(x^n - 1) = x^{[mn]} - x$. Moreover, in such case $F^(x) = F_*(x)$, $F^0(x) = F_0(x)$ and $F^\perp(x) = F^\top(x)$, and coincide by the previous ring isomorphism to the definitions in (4), (5) and (6), respectively.*

Hence the results in this section give those in the previous one that have to do with divisibility of generator and check polynomials. However, the root description will be essentially different. As we will see, it will not be necessary to assume that q and n are coprime, and finding roots of linearized polynomials can always be done efficiently (see [11, Chapter 3]).

Before going on, we will establish a result analogous to Proposition 3. In the linearized case, if $G(x)$ and $H(x)$ are coprime on both sides, then there exist an idempotent generator $E(x)$ of C by [12, Theorem 2], and the linear skew cyclic code with generator and check polynomials $H(x)$ and $G(x)$, respectively, is a complementary space of C by [12, Proposition 5]. We denote it by C^c . It also has an idempotent generator given by $x - E(x)$ [12, Proposition 5].

Proposition 7. *The following are equivalent:*

1. C is Galois closed.
2. $G(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$.
3. $H(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$.
4. $Z(G) \subseteq \mathbb{F}_{q^{rn}}$ is an $(\mathbb{F}_{q^r}$ -linear) Galois closed space over \mathbb{F}_q . That is, $Z(G)^q = Z(G)$ (also called q -modulus in [11, Chapter 3]).
5. (If $G(x)$ and $H(x)$ are coprime on both sides) $E(x) \in \mathbb{F}_q[x]$.
6. (If $G(x)$ and $H(x)$ are coprime on both sides) C^c is Galois closed.

Proof. Analogous to that of Proposition 3. \square

It is proven in [2, 5, 6] that $H^\perp(x)$ is the generator polynomial of C^\perp . We now find its check polynomial:

Lemma 6. *The check polynomial of C^\perp is $G^\top(x)$.*

Proof. Let $\tilde{G}(x) = \tilde{G}_0x + \tilde{G}_1x^{[r]} + \dots + \tilde{G}_{n-k}x^{[(n-k)r]}$ be the check polynomial of C^\perp . It is shown in [2] that C^\perp has a parity check matrix of the form

$$\begin{pmatrix} G_0 & G_1 & \dots & G_{n-k} & 0 & \dots & 0 \\ 0 & G_0^{[r]} & \dots & G_{n-k-1}^{[r]} & G_{n-k}^{[r]} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & G_0^{[(k-1)r]} & G_1^{[(k-1)r]} & \dots & G_{n-k}^{[(k-1)r]} \end{pmatrix}.$$

By [12, Theorem 1, items 4 and 6], there is a unique parity check matrix of that form and hence it holds that $\tilde{G}_i^{[(n-k+i)r]} = G_{n-k-i}/G_0$. Raising this equality to the power $[(k+i)r]$ we obtain $\tilde{G}_i = \tilde{G}_i^{[nr]} = (G_{n-k-i}/G_0)^{[(k+i)r]}$, for $i = 0, 1, 2, \dots, n-k$, since m divides rn , and we are done. \square

On the other hand, we have the following:

Lemma 7. *For a q^r -polynomial $F(x) = F_0x + F_1x^{[r]} + \dots + F_dx^{[rd]} \in \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ that divides $x^{[rn]} - x$, with $F_d \neq 0$, it holds that*

$$F^{\perp\top}(x) = F^{\top\perp}(x) = F(x)/F_d,$$

$$(F_*)^\perp(x) = (F^\perp)^*(x) \quad \text{and} \quad (F_0)^\perp(x) = (F^\perp)^0(x),$$

and analogously replacing \perp by \top in the last two equalities.

Proof. The first two equalities are straightforward computations. For the last two equalities, it is enough to observe again that $\theta_i(F^\perp(x)) = \theta_i(F(x))^\perp$ and use the previous two equalities. Analogously replacing \perp by \top . \square

We will need the following result, which is [12, Theorem 4]:

Lemma 8 ([12, Theorem 4]). *Assume that $C_1, C_2 \subseteq \mathbb{F}_{q^m}^n$ are linear q^r -cyclic codes with generator polynomials $G_1(x)$ and $G_2(x)$, respectively. Then*

1. $C_1 \cap C_2$ is the q^r -cyclic code with generator polynomial $M(x) = \text{lcm}(G_1(x), G_2(x))$ and $Z(M) = Z(G_1) + Z(G_2)$.
2. $C_1 + C_2$ is the q^r -cyclic code with generator polynomial $D(x) = \text{gcd}(G_1(x), G_2(x))$ and $Z(D) = Z(G_1) \cap Z(G_2)$.

Finally, we may compute the generator and check polynomials of C^* and C^0 , seen as q^r -cyclic codes:

Proposition 8. *The generator and check polynomials of C^* are $G^*(x)$ and $H_0(x)$, respectively, and the generator and check polynomials of C^0 are $G^0(x)$ and $H_*(x)$, respectively.*

Proof. By the previous lemma, if $C_1, C_2 \subseteq \mathbb{F}_{q^m}^n$ are q^r -cyclic codes with generator polynomials $G_1(x), G_2(x)$, respectively, and check polynomials $H_1(x), H_2(x)$, respectively, it holds that $C_1 + C_2$ and $(C_1 + C_2)^\perp = C_1^\perp \cap C_2^\perp$ have generator polynomials $\gcd(G_1(x), G_2(x))$ and $\text{lcm}(H_1^\perp(x), H_2^\perp(x))$ (on the right), respectively. By the previous lemma and Lemma 6, the check polynomial of $C_1 + C_2$ is then $\text{lcm}(H_1^\perp(x), H_2^\perp(x))^\top$.

We obtain the result for C^* by applying this iteratedly to $C, \theta_1(C), \theta_2(C), \dots, \theta_{m-1}(C)$, observing that the generator and check polynomials of $\theta_i(C)$ are $\theta_i(G(x))$ and $\theta_i(H(x))$, respectively, for $i = 0, 1, 2, \dots, m-1$. Similarly for C^0 . \square

We know from Lemma 2 that C^* and C^0 are skew cyclic of all orders. In the previous sections we used their cyclic (or q^0 -cyclic) nature and their conventional generator and check polynomials. We may relate them with the generator and check polynomials obtained in the previous proposition.

For that purpose, we define the operator $L : \mathbb{F}_{q^m}[x] \longrightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ by

$$L(f_0 + f_1x + \dots + f_dx^d) = f_0x + f_1x^{[r]} + \dots + f_dx^{[rd]}, \quad (15)$$

which coincides with the map in (14) for $r = m$.

Proposition 9. *Let the notation be as in the previous proposition, and let $g^*(x), g^0(x)$ be the generator (conventional) polynomials of C^* and C^0 , respectively, and let $h^0(x)$ and $h^*(x)$ be their check (conventional) polynomials, respectively. Then*

$$\begin{aligned} G^*(x) &= L(g^*(x)), & H_0(x) &= L(h^0(x)), \\ G^0(x) &= L(g^0(x)), & \text{and } H_*(x) &= L(h^*(x)). \end{aligned}$$

Proof. It follows from the uniqueness of the generator and parity check matrices for cyclic and q^r -cyclic codes given by their generator and check polynomials. See [8, Theorem 4.2.1 and Theorem 4.2.7] for the cyclic case, and [2] and [12, Theorem 1] for the q^r -cyclic case. \square

On the other hand, we have the following relations between the root spaces of the generator and check polynomials of C, C^* and C^0 , as in Proposition 6.

Proposition 10. *It holds that*

1. $Z(G^*) = \bigcap_{i=0}^{m-1} Z(G)^{[i]}$ and $Z(G^0) = \sum_{i=0}^{m-1} Z(G)^{[i]}$.
2. $\dim_{\mathbb{F}_{q^r}}(Z(H_*)) = \dim_{\mathbb{F}_{q^r}}(\bigcap_{i=0}^{m-1} Z(H^\perp)^{[i]})$.
3. $\dim_{\mathbb{F}_{q^r}}(Z(H_0)) = \dim_{\mathbb{F}_{q^r}}(\sum_{i=0}^{m-1} Z(H^\perp)^{[i]})$.

Proof. The first item follows from Lemma 8 and the fact that $Z(\theta_i(G)) = Z(G)^{[i]}$, for $i = 0, 1, 2, \dots, m-1$.

On the other hand, since $H_*(x)$ divides $x^{[rn]} - x$ on the right, it also divides it conventionally, and hence it has simple roots. Hence it holds that $\dim_{\mathbb{F}_{q^r}}(Z(H_*)) = \deg_{q^r}(H_*(x))$ and similarly for $(H_*)^\perp(x)$. Thus

$$\dim_{\mathbb{F}_{q^r}}(Z(H_*)) = \deg_{q^r}(H_*(x)) = \deg_{q^r}((H_*)^\perp(x)) = \dim_{\mathbb{F}_{q^r}}(Z((H_*)^\perp)).$$

Again by Lemma 8 and Lemma 7, we have that

$$Z((H_*)^\perp) = \bigcap_{i=0}^{m-1} Z(H^\perp)^{[i]},$$

using again the fact that $Z(\theta_i(H^\perp)) = Z(H^\perp)^{[i]}$, for $i = 0, 1, 2, \dots, m-1$. Therefore item 2 follows. Item 3 is proven in a similar way. \square

We may now state a similar result to Theorem 3:

Theorem 4. *It holds that*

$$\begin{aligned} l_R(C) &= n - \deg_{q^r}(\gcd(G(x), \theta_1(G(x)), \dots, \theta_{m-1}(G(x)))) \\ &= \deg_{q^r}(\text{lcm}(H^\perp(x), \theta_1(H^\perp(x)), \dots, \theta_{m-1}(H^\perp(x)))) \\ &= n - \dim_{\mathbb{F}_{q^r}} \left(\bigcap_{i=0}^{m-1} Z(G)^{[i]} \right) = \dim_{\mathbb{F}_{q^r}} \left(\sum_{i=0}^{m-1} Z(H^\perp)^{[i]} \right). \end{aligned}$$

Proof. The first two equalities follow from Theorem 2, item 1, and Proposition 9. The next two equalities follow from the previous proposition and the fact that $\dim_{\mathbb{F}_{q^r}}(Z(G^*)) = \deg_{q^r}(G^*(x))$ and $\dim_{\mathbb{F}_{q^r}}(Z(H_0)) = \deg_{q^r}(H_0(x))$, since they have simple roots. \square

Now we obtain the following characterizations of rank degenerate skew cyclic codes:

Corollary 4. *The following conditions are equivalent:*

1. C is rank degenerate. That is, $l_R(C) < n$.
2. $\gcd(G(x), \theta_1(G(x)), \dots, \theta_{m-1}(G(x))) \neq x$.
3. $\text{lcm}(H^\perp(x), \theta_1(H^\perp(x)), \dots, \theta_{m-1}(H^\perp(x))) \neq x^{[rn]} - x$.
4. $\bigcap_{i=0}^{m-1} Z(G)^{[i]} \neq \{0\}$.
5. $\sum_{i=0}^{m-1} Z(H^\perp)^{[i]} \neq \mathbb{F}_{q^{rn}}$.
6. $G(x)$ is divisible on the right by some polynomial $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$ in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ with $\deg_{q^r}(F(x)) > 0$.
7. $H(x)$ divides on the right some polynomial $F(x) \in \mathcal{L}_{q^r}\mathbb{F}_q[x]$ in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$ with $\deg_{q^r}(F(x)) < n$.

7 Attaining the rank length by pseudo-skew cyclic codes

So far we have tried to find the linear skew cyclic code of smallest length that is rank equivalent to a given one C . We have given upper bounds on that length and seen that a general lower bound is $l_R(C)$, although it is not clear that this length can be attained by a linear skew cyclic code that is rank equivalent to C .

On the other hand, in this section we will see that the length $l_R(C)$ is always attained by some linear pseudo-skew cyclic code. As skew cyclic codes, pseudo-skew cyclic codes were introduced in [5] for $r = 1$ and $n = m$, and then independently in [6] for $r = 1$ and in [2] for general parameters. They are not invariant by q^r -shifting operators, but have similar conventional-polynomial and linearized-polynomial representations.

We start by defining the well-known pseudo-cyclic codes:

Definition 4. Let $f(x) \in \mathbb{F}_{q^m}[x]$ be of degree n . For a linear code $C \subseteq \mathbb{F}_{q^m}^n$, we define $C_{f(x)}(x)$ as the image of C in $\mathbb{F}_{q^m}[x]/(f(x))$ by the linear vector space isomorphism $\mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}[x]/(f(x))$ given by

$$(c_0, c_1, \dots, c_{n-1}) \mapsto c_0 + c_1x + \dots + c_{n-1}x^{n-1}.$$

Then we say that C is pseudo-cyclic if $C_{f(x)}(x)$ is an ideal in $\mathbb{F}_{q^m}[x]/(f(x))$, for some $f(x) \in \mathbb{F}_{q^m}[x]$ of degree n .

Fix now a linear cyclic code $C \subseteq \mathbb{F}_{q^m}^n$, and let the notation be as in Section 5. We have the following:

Theorem 5. *The map $\phi : \mathbb{F}_{q^m}[x]/(h^0(x)) \longrightarrow (g^*(x))/(x^n - 1)$ given by*

$$\phi(f(x)) = f(x)g^*(x)$$

is well-defined, maps ideals to ideals and constitutes a rank equivalence when seeing its domain and codomain as linear Galois closed spaces.

Proof. First of all, it is well-defined since $h^0(x)g^*(x) = x^n - 1$. It is linear since it preserves additions and $\phi(p(x)f(x)) = p(x)\phi(f(x))$, for all $p(x), f(x) \in \mathbb{F}_{q^m}[x]$. For the same reason it maps ideals to ideals.

On the other hand, if $f(x)g^*(x) = 0$ in the quotient $(g^*(x))/(x^n - 1)$, then $f(x)g^*(x) = p(x)(x^n - 1)$ for some polynomial $p(x) \in \mathbb{F}_{q^m}[x]$, which implies that $f(x) = p(x)h^0(x)$. Therefore, ϕ is one to one. Since it is obviously onto, we conclude that it is a vector space isomorphism.

Finally, since $g^*(x) \in \mathbb{F}_q[x]$, we see that ϕ maps polynomials of degree less than k with coefficients in \mathbb{F}_q to polynomials with coefficients in \mathbb{F}_q , and hence it is a rank equivalence by Lemma 1. \square

Therefore the following consequence follows immediately:

Corollary 5. *The length $l_R(C)$ is attained by a linear pseudo-cyclic code that is an ideal in the quotient ring $\mathbb{F}_{q^m}[x]/(h^0(x))$.*

Remark 8. If $h^0(x) = x^e - 1$, for some positive integer e , then the pseudo-cyclic code in the previous corollary is actually cyclic. This also follows from Remark 5.

In a completely analogous way, we may state similar results for the general skew cyclic case. However, in this case we may only construct quotient rings with two-sided ideals, since the ring of linearized polynomials is not commutative. For that purpose, we consider the center of $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]$, denoted by $\mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ and defined as the set of q^r -polynomials over \mathbb{F}_{q^m} that commute with every other q^r -polynomial over \mathbb{F}_{q^m} . It is well-known that

$$\mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]) = \mathcal{L}_{q^l}\mathbb{F}_{q^d}[x],$$

where $l = \text{lcm}(m, r)$ and $d = \text{gcd}(m, r)$. We may now proceed exactly as in the conventional case:

Definition 5. Let $F(x) \in \mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ such that $\deg_{q^r}(F(x)) = n$. For a linear code $C \subseteq \mathbb{F}_{q^m}^n$, we define $C_{F(x)}(x)$ as the image of C in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$ by the linear vector space isomorphism $\mathbb{F}_{q^m}^n \rightarrow \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$ given by

$$(c_0, c_1, \dots, c_{n-1}) \mapsto c_0x + c_1x^{[r]} + \dots + c_{n-1}x^{[(n-1)r]}.$$

Then we say that C is pseudo-skew cyclic (of order r) if $C_{F(x)}(x)$ is a left ideal in $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(F(x))$, for some $F(x) \in \mathbb{C}(\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x])$ such that $\deg_{q^r}(F(x)) = n$.

Fix now a linear q^r -cyclic code $C \subseteq \mathbb{F}_{q^m}^n$, and let the notation be as in Section 6. We have the following:

Theorem 6. Assume that $H_0(x)$ is central. Then the map $\phi : \mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(H_0(x)) \rightarrow (G^*(x))/(x^{[rn]} - x)$ given by

$$\phi(F(x)) = F(x) \otimes G^*(x)$$

is well-defined, maps left ideals to left ideals and constitutes a rank equivalence when seeing its domain and codomain as linear Galois closed spaces.

Proof. Analogous to that of Theorem 5, taking into account the non-commutativity of the symbolic product of linearized polynomials. \square

Hence the following consequence follows immediately:

Corollary 6. If $H_0(x)$ is central, then the length $l_R(C)$ is attained by a linear pseudo-skew cyclic code that is a left ideal in the quotient ring $\mathcal{L}_{q^r}\mathbb{F}_{q^m}[x]/(H_0(x))$.

Acknowledgement

The author wishes to thank Olav Geil and Diego Ruano for fruitful discussions and careful reading of the manuscript. The author also gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367).

References

- [1] D. Boucher, W. Geiselmann, and F. Ulmer. Skew-cyclic codes. *Applicable Algebra in Engineering, Communication and Computing*, 18(4):379–389, 2007.
- [2] D. Boucher and F. Ulmer. Coding with skew polynomial rings. *Journal of Symbolic Computation*, 44(12):1644 – 1656, 2009. Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics.
- [3] J. Ducoat. Generalized rank weights: a duality statement. *Topics in Finite Fields*, 632:101 – 109, 2015.
- [4] J. Ducoat and F. Oggier. Rank weight hierarchy of some classes of cyclic codes. In *Information Theory Workshop (ITW), 2014 IEEE*, pages 142–146, 2014.
- [5] E. M. Gabidulin. Theory of codes with maximum rank distance. *Problems Information Transmission*, 21, 1985.
- [6] E. M. Gabidulin. Rank q-cyclic and pseudo-q-cyclic codes. In *IEEE International Symposium on Information Theory, 2009. ISIT 2009.*, pages 2799–2802, 2009.
- [7] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov. Ideals over a non-commutative ring and their application in cryptology. In Donald W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, volume 547 of *Lecture Notes in Computer Science*, pages 482–489. Springer Berlin Heidelberg, 1991.
- [8] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.
- [9] R. Jurrius and R. Pellikaan. On defining generalized rank weights. *arXiv:1506.02865*, 2015.
- [10] J. Kurihara, R. Matsumoto, and T. Uyematsu. Relative generalized rank weight of linear codes and its applications to network coding. *IEEE Transactions Information Theory*, 61(7):3912–3936, July 2015.
- [11] R. Lidl and H. Niederreiter. *Finite Fields*, volume 20. Encyclopedia of Mathematics and its Applications. Addison-Wesley, Amsterdam, 1956.
- [12] U. Martínez-Peñas. On the roots and minimum rank distance of skew cyclic codes. *arXiv:1511.09329*, 2015.
- [13] U. Martínez-Peñas. On the similarities between generalized rank and Hamming weights and their applications to network coding. *arXiv:1506.04036*, 2015.
- [14] O. Ore. On a special class of polynomials. *Transactions American Mathematical Society*, 35(3):559–584, 1933.

- [15] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics (2)*, 34(3):480–508, 1933.
- [16] D. Silva and F. R. Kschischang. On metrics for error correction in network coding. *IEEE Transactions Information Theory*, 55(12):5479–5490, 2009.
- [17] H. Stichtenoth. On the dimension of subfield subcodes. *IEEE Transactions Information Theory*, 36(1):90–93, 1990.